CPTE - Certified Penetration Testing Engineer

Course Overview

This course teaches students special knowledge and skills in penetration testing. Topics covered include reconnaissance, hacking operating systems, evasion techniques, hacking with PowerShell, mobile and IoT hacking, report writing, and more.

Module 1 - Business and Technical Logistics for Pen Testing 1h 55m

Course Introduction
Business and Technical Logistics for Pen Testing
Where are We?
Overview
Section 1: What is Penetration Testing?
What is a Penetration Test?
Risk Management Flow
Risk Management Reference Documents
NIST SP 800-39 Risk Context
Risk Management and Penetration Testing
One Main Reason we NEED a Penetration Test?
Requirements for Pentest
Requirements for Pentest
Requirements for Pentest
Benefits of a Penetration Test
What Does a Hack Cost You?
2017 Annual Report
2017 Crime Type
2017 Crime Type
2017 Annual Report
Types of Penetration Testing
Types of Penetration Tests
Section 2: Today's Threats
Who/Why/Skills
Exploit and Vulnerability Lifecycle
Zero Day Anyone?
2017 Verizon Data Breach Report
2017 Verizon Data Breach Report
2017 Symantec ISTR
2017 Symantec ISTR Supply Chain Attacks
2017 Symantec ISTR Top Threats
2017 Symantec ISTR Top Threats
2017 Symantec ISTR Top Threats
2017 Symantec ISTR Top Threats
2017 Symantec ISTR Vulnerabilities
2017 Symantec ISTR IoT
Section 3: Staying Up To Date

Stay Up to Date
Website Review General Security
Website Review Statistics/Threat Level/Maps
Website Review Penetration Testing
Section 4: Pen Testing Methodology
Options
Penetration Testing Methodologies
OSSTMM
OSSTMM – The Trifecta
OSSTMM Combining Trifecta and 4PP
NIST SP-800-115
NIST SP-800-115
ISSAF Four Phases
ISSAF
PTES
Methodology for Penetration Testing
So Which One?
Not Just Tools
Section 5: Phase 1 – Pre-Engagement Activities
Where are we in the Process?
Components of Phase 1
Scope and Time
Asking Questions
What can we do?
Communication
Goals
Rules of Engagement
Stay Legal
Review

Module 2 - Information Gathering – Reconnaissance-Passive (External Only) 56m

Information Gathering – Reconnaissance-Passive (External Only)
Where are We?
Overview
Section 1: What are we looking for?
Where are we in the Process?
What is it?
Open-Source Intelligence (OSINT)
OSINT Framework
Why do we do it?
What do we want?
What do we want?
What do we want?
What do we want?
Section 2: Keeping Track of what we find!
Can you remember everything?
Free Mind Mapping Tools
Section 3: Where/How do we find this information?
Where?
Where Do We Find This Information?

Domain Name Registration
WHOIS
Whois Info – mile2.com
DNS Databases
Using Nslookup
Username Searches
eMail Address Searches
Social Networks
Social Network Apps
People Search Engines
Business Search Engines
Client Email Reputation
Web Server Info Tool: Netcraft
Internet Archive: The WayBack Machine
Job Postings
Blogs & Forums
Shodan
Censys
Google Hacking
GHDB
Section 4: Are there tools to help?
Maltego – Clear Leader
Maltego – Clear Leader
Recon-ng
Recon-ng
theharvester
Firecat/Kromcat
Section 5: Countermeasures
Policies
Countermeasures
Information Gathering Countermeasures
DOMAINSBYPROXY.COM
Review

Module 3 - Detecting Live Systems – Reconnaissance-Active 1h 6m

Detecting Live Systems – Reconnaissance-Active
Where are We?
Overview
Section 1: What are we looking for?
Where are we in the Process?
What is it?
What are we looking for?
Methods of Obtaining Information
Section 2: Reaching Out!
Physical Access
On-Location Gathering Penetration Testing Execution Standard
Social Access
Social Engineering Techniques
Additional SE Techniques
Popular SE Tool

Section 3: Port Scanning
Introduction to Port Scanning
Which Services use Which Ports?
Legalities
Port Scan Tips
Port Scans Should Reveal…
Comparison of Models
Types of Scans
TCP/IP Suite
TCP Flags
TCP 3-Way Handshake
TCP Connect Port Scan
Half-open Scan (SynScan)
Firewalled Ports
UDP versus TCP
UDP Port Scan
Section 4: Are there tools to help?
Popular Port Scanning Tools
Stealth Online Ping
Online Tools
Fing & Fing mobile
Solarwinds Port Scanner
Hping3
Hping3
Hping3
P0f
NMAP: Is the Host online?
ICMP Disabled?
NMAP TCP Connect Scan
Nmap (cont.)
Tool Practice: TCP Half-open & Ping Scan
NMAP Service Version Detection
Additional NMAP Scans
Saving NMAP results
NMAP UDP Scans
Advanced Technique
Section 5: Countermeasures
Countermeasures: Scanning
Social Engineering Countermeasures
Review

Module 4 - Banner Grabbing & Enumeration 45m
Banner Grabbing & Enumeration
Overview
Section 1: Banner Grabbing
Introduction
Why Banner Grabbing?
Active Banner Grabbing
Passive Banner Grabbing
Banner Grabbing Tools

Banner Grabbing Tools – ID Serve
Banner Grabbing Tools - Netcraft
Banner Grabbing Tools - Netcat
Banner Grabbing Tools - Telnet
Practice: Banner Grabbing with Telnet
Banner Grabbing Tools - NMAP
Banner Grabbing Tools - NMAP
CURL
Dmitry
Countermeasures
Section 2: Enumeration
Enumeration
Services to Enumerate:
SNMP
SNMP Countermeasures
LDAP
LDAP Countermeasures
NTP
SMTP
SMTP Countermeasures
SMTP Countermeasures
SMTP Countermeasures
DNS
DNS Countermeasures
Review

Module 5 - Automated Vulnerability Assessment 27m

Automated Vulnerability Assessment
Where are we?
Overview
Section 1: What is a Vulnerability Assessment?
Review from CSP+
What is a Vulnerability Assessment (VA)?
Benefits of a Vulnerability Assessment
Requirements for Vulnerability Assessments
Requirements for Vulnerability Assessments
Requirements for Vulnerability Assessments
Types of Vulnerability Assessments
How do we know about Vulnerabilities?
CVE Example
NVD Example
NVD Example
NVD Example
Typical Vulnerability Assessment Process
Section 2: Tools of the Trade
Choosing the Right Tool
Different Types of Tools
The List
Network Based Tools Comparison
Application Based Tools Comparison

Section 3: Testing Internal/External Systems
It starts here!
Enumeration
Detection
Additional Details
Section 4: Dealing with the Results
The Report
Results for Pentests
Example of a report from Rapid7 Nexpose
Results for Maintaining Security
Patching Tools
Review

Module 6 - Hacking Operating Systems 1h 25m
Hacking Operating Systems
Where are We?
Overview
Section 1: Key Loggers
Introduction
Spyware by Definition
What is and is not Spyware
Spyware Distribution
Spyware Distribution
Spyware Activities
Keyloggers by Definition
Hardware Keyloggers
Log of a Hardware Keylogger
Software Keylogger
Types of Software Keyloggers
Windows Keylogger
Amac
Linux Keyloggers
Kernel/Driver Keyloggers
Kernel/Driver Keyloggers
Method of Infection
Countermeasures
Countermeasures
Countermeasures
Section 2: Password Attacks
Password Guessing
General Password Policies
Password Cracking LM/NTLM Hashes
Syskey Encryption
Cracking Techniques
Cain and Abel's Cracking Methods
GPU or CPU for Password Cracking
NTPASSWD: Hash Insertion Attack
Password Sniffing
Windows Authentication Protocols
Mimikatz

A few other common tools
Countermeasures: System Encryption
Countermeasures: Tokens & Smart Cards
Smart Cards
Section 3: Rootkits & Their Friends
RootKit
Windows RootKit Countermeasures
Hiding Files with NTFS Alternate Data Stream
NTFS Streams Countermeasures
Stream Explorer
What is Steganography?
Steganography Tools
Section 4: Clearing Tracks
Covering Tracks Overview
Disabling Auditing
Log Editing in Windows
Clearing Event Log
Clearing Event Logs
Windows Log Tricks
WinZapper - A Few Clutzy Examples
WinZapper
MRU
Meterpreter Log File Alterations
Linux Bash History
Linux Bash History
Linux Log Files
Shredding Files Left Behind
Shredding Files Left Behind
More Anonymous Software
Anonymous Internet Access
Anonymous Browsing
Private Browsing
Leaving No Local Trace
Defenses or Counter Measures
Defenses or Counter Measures for Covering your Tracks
Review

Module 7 - Advanced Assessment and Exploitation Techniques 30m
Advanced Assessment and Exploitation Techniques
Where are We?
Overview
Section 1: Buffer Overflow
Introduction to Buffer overflow
Stack
Stack-based Buffer Overflow
Stack-based Buffer Overflow Cont'd
Heap
Heap-Based Buffer Overflow
Overflow Using Format String
Why Programs and Applications are Vulnerable to Buffer Overflows?

Buffer Overflow - Program Related Issues
Handling Buffer Overflow Exploits - Knowhow
Steps to Handle Buffer Overflow
Section 2: Exploits
What is an Exploit?
Exploit Development
Exploit Development
Section 3: Exploit Framework
Metasploit
Metasploit
Understanding Metasploit
Penetration Testing with Metasploit
Hands on Metasploit
Exploits
Auxiliary
Payload
Options
Options
Core Impact
Core Impact
SaintExploit at a Glance
Review

Module 8 - Evasion Techniques 33m
Evasion Techniques
Where are We?
Overview
Section 1: Evading Firewall
Evading Firewall-IP Address Spoofing
Evading Firewall-Source Routing
Evading Firewalls- Tiny Fragments
Evading Firewalls-Bypass Blocked Sites Using IP Address
Evading Firewalls-Anonymous Website Surfing Sites
Evading Firewalls-Proxy Server
Evading Firewalls-ICMP Tunneling
Evading Firewalls-ACK Tunneling
Evading Firewalls-HTTP Tunneling
Evading Firewalls-External Systems
Evading Firewalls-MITM Attack
Firewall Evasion Tool-Traffic IQ Professional
Firewall Evasion Tool-TCP OVER DNS
Section 2: Evading Honeypots
Honeypot
Types of Honeypots
Detecting Honeypots
Honeypot Detection Tool -Send-Safe Honeypot Hunter
Countermeasures
Firewall Penetration Testing
Section 3: Evading IDS
Introduction

Intrusion Detection Systems
Evading IDS
Encryption and Flooding
Obfuscating
Fragmentation Attack
Fragmentation Attack Cont'd
Overlapping Fragments
Vulnerability in IDS
Insertion Attack
Evasion
Denial-of-Service Attack
Application-Layer Attacks
Time-To-Live Attacks
False Positive Generation
Urgency Flag
Session Splicing
Desynchronization - Pre Connection SYN
Desynchronization - Post Connection SYN
Ways to Detect
IDS Evading Tool: ADMutate
Countermeasures
Review

Module 9 - Hacking with PowerShell 17m
Hacking with PowerShell
Where are We?
Overview
Section 1: PowerShell - A Few Interesting Items
Systems supporting PowerShell
PowerShell Users
Interesting Information
What Parts of Pen Testing can we do with Powershell?
Any User?
Commands to Start With!
A Few Interesting Items
A Few Interesting Items
Get-ADComputer
A Few Interesting Items
Section 2: Finding Passwords with PS
Guessing Domain Passwords
Creating a New Object
dsquery
dsquery
PowerShell and USB
Commercial Example
The Basics with Rubber Ducky
Review

Module 10 - Networks, Sniffing, and IDS 19m

Networks, Sniffing, and IDS
Where are We?
Overview
Section 1: Sniffing Techniques
Packet Sniffers
Example Packet Sniffers
Tool: Pcap & WinPcap
Tool: Wireshark
TCP Stream Re-assembling
tcpdump & windump
TCPdump examples
Sniffer Detection using Cain & Abel
Passive Sniffing
Active Sniffing
Active Sniffing Methods
Switch Table Flooding
ARP Cache Poisoning
ARP Normal Operation
ARP Cache Poisoning
Technique: ARP Cache Poisoning (Linux)
MAC Spoofing
DNS Poisoning
Source Routing
Advertise Bogus Routes
Rogue DHCP
Tool: Cain and Abel
Ettercap
Linux Tool Set:Dsniff Suite
What is DNS Spoofing?
Tools: DNS Spoofing
Breaking SSL Traffic
Breaking SSL Traffic
URL Obfuscation
Intercepting VoIP
Countermeasures
Countermeasures
Countermeasures for Sniffing
Review

Module 11 - Assessing and Hacking Web Technologies 37m

Assessing and Hacking Web Technologies
Where are We?
Overview
Section 1: OWASP Top 10
OWASP Top 10
A1 - Injection
A2 - Broken Authentication
A3 - Sensitive Data Exposure
A4 - XML External Entities (XXE)

A5 - Broken Access Control
A6 - Security Misconfiguration
A7 - Cross-Site Scripting
A8 - Insecure Deserialization
A9 - Using Components with Known Vulnerabilities
A10 - Insufficient Logging and Monitoring
Section 2: SQL Injection
Introduction
SQL Injection Attack Characters
Types of Signature Evasion Techniques
SQL Injection Methodology
SQL Injection Methodology Cont'd
Advanced SQL Injection Steps
SQL Injection Attacks
Types of SQL Injection
Blind SQL Injection
Simple SQL Injection Attack
Union & Error Based SQL Injection
Evasion Technique
SQL Injection Detection
SQL Injection Tools
SQL Injection Tools Cont'd
SQL Injection Tools Cont'd
Testing for SQL Injection
Countermeasures
SQL Injection Detection Tool
SQL Injection Detection Tool Cont'd
SQL Injection Detection Tool Cont'd
SQL Injection Detection Tool Cont'd
Section 3: XSS
Cross-Site Scripting (XSS/CSS)
Introduction to Cross-Site Scripting
Type of XSS
Stored XSS or Persistent/Type I)
Reflected XSS (Non-Persistent or Type II)
DOM Based XSS (Type-0)
Server XSS
Client XSS
XSS Types in the Matrix
Preventing XSS
Browser Behaviors that Lead to XSS
OWASP Rules
OWASP Rules
OWASP Rules
OWASP Rules
Test for XSS Vulnerability
Code Review
Web Application Security Scanners
Testing
Review

Module 12 - Mobile and IoT Hacking 54m

Mobile and IoT Hacking
Where are We?
Overview
Quick Introduction
Section 1: What Devices are we talking about?
Definitions
Number of Mobile Devices
Mobile OS Market Share
Number of IoT Devices
Mobile/IoT Devices
What Makes IoT Unique?
Section 2: What is the risk?
What is the Big Deal?
Trend Micro 2017 Mobile Threat Landscape
Trend Micro 2017 Mobile Threat Landscape
Trend Micro 2017 Mobile Threat Landscape
Risks and Threats Mobile Devices
Risks and Threats Mobile Devices
Security Incidents Attributable to IoT
Top 5 IoT Hacks
New IoT Botnet Offers DDoSes of Once-Unimaginable Sizes for $20
IoT Risks and Threats
Section 3: Potential Avenues to Attack
Nothing New
What to Consider - Mobile Devices
What to Consider - Mobile Devices
Bluetooth Tools for Attacking
Some Bluetooth Attacks
What to Consider - IoT
Section 4: Hardening Mobile/IoT Devices
Areas to Consider
Device Security
Device Security
Application Security
Application Security
Mobile Device Connections to Secure
Hardening the Devices
Is IoT Any Different?
Security Areas that Apply to IoT
General Hardening Recommendations for IoT
Implement IoT Standards
Review

Module 13 - Report Writing Basics 37m

Report Writing Basics
Where are We?
Overview
Section 1: Report Components
Additional Items

The Report
Report Criteria: Supporting Documentation
Analyzing Risk
Analyzing Risk
Section 2: Report Results Matrix
Report Results Matrix
Findings Matrix
Findings Matrix
Findings Matrix
Findings Matrix
Delivering The Report
Delivering The Report
Stating Fact
Section 3: Recommendations
Recommendations
Recommendations
Executive Summary
Technical Report
Report Table Of Contents
Summary Of Security Weaknesses Identified
Scope of Testing
Summary Recommendations
Summary Observations
Detailed Findings
Detailed Findings
Strategic and Tactical Directives
Statement of Responsibility/Appendices
Review
Course Review

Total Duration: 10h 23m